

Docket No. 2001-088-NSC

CLAIMS:

What is claimed is:

- 1 1. A method of upgrading the integrity of a first
2 timestamp having a first digital signature, the method
3 comprising:
4 computing a hash value of the first digital
5 signature;
6 combining the hash value with a current time value
7 to form a second data item;
8 computing a second digital signature based on the
9 second data item; and
10 combining the second data item and the second
11 digital signature to form a second timestamp.
- 1 2. The method of claim 1, wherein computing the hash
2 value, combining the hash value with the current time
3 value, computing the second digital signature, and
4 combining the second data item and the second digital
5 signature are performed in response to a determination
6 that the integrity of the first digital signature may
7 soon become able to be compromised.
- 1 3. The method of claim 1, further comprising writing
2 the second timestamp to a storage medium.
- 1 4. The method of claim 3, further comprising writing
2 the first timestamp to the storage medium.

2003-11-13 14:34:11

Docket No. 2001-088-NSC

1 5. The method of claim 3, wherein the storage medium is
2 memory.

1 6. The method of claim 3, wherein the storage medium is
2 one of a disk and tape.

1 7. A method of upgrading the integrity of a first
2 timestamp of a document, wherein the first timestamp
3 includes a first hash value computed with a first hash
4 function, the method comprising:
5 calculating a second hash value of the document
6 using a second hash function;
7 combining the second hash value with a current time
8 value to form a data item;
9 computing a digital signature of the data item; and
10 combining the digital signature and the data item to
11 form a second timestamp.

1 8. The method of claim 7, wherein computing the second
2 hash value, combining the second hash value with the
3 current time value, computing the digital signature, and
4 combining the data item with the digital signature are
5 performed in response to a determination that the
6 integrity of the first hash value may soon become able to
7 be compromised.

1 9. The method of claim 7, further comprising writing
2 the second timestamp to a storage medium.

Docket No. 2001-088-NSC

1 10. The method of claim 9, further comprising writing
2 the first timestamp to the storage medium.

1 11. The method of claim 9, wherein the storage medium is
2 memory.

1 12. The method of claim 9, wherein the storage medium is
2 one of a disk and tape.

1 13. A method of verifying the integrity of an upgrade
2 timestamp associated with an earlier timestamp,
3 comprising:
4 verifying integrity of a first digital signature
5 associated with the upgrade timestamp;
6 calculating a first hash value of a second digital
7 signature associated with the earlier timestamp; and
8 verifying that the first hash value matches a second
9 hash value associated with the upgrade timestamp.

1 14. The method of claim 13, further comprising:
2 verifying integrity of the earlier timestamp.

1 15. The method of claim 14, wherein verifying the
2 integrity of the earlier timestamp includes:
3 verifying integrity of the second digital signature;
4 calculating a third hash value of a document
5 associated with the earlier timestamp; and
6 verifying that the third hash value matches a fourth
7 hash value associated with the earlier timestamp.

Docket No. 2001-088-NSC

1 16. A method comprising:

2 verifying integrity of each of a plurality of
3 digital signatures, wherein each of the plurality of
4 digital signatures signs a timestamp, and each timestamp
5 includes a hash value of a common document, each hash
6 value having been calculated with a different hash
7 function.

1 17. A computer program product in a computer readable
2 medium for upgrading the integrity of a first timestamp
3 having a first digital signature, comprising functional
4 descriptive data that, when executed by a computer,
5 enables the computer to perform acts including:

6 computing a hash value of the first digital
7 signature;

8 combining the hash value with a current time value
9 to form a second data item;

10 computing a second digital signature based on the
11 second data item; and

12 combining the second data item and the second
13 digital signature to form a second timestamp.

1 18. The computer program product of claim 17, wherein
2 computing the hash value, combining the hash value with
3 the current time value, computing the second digital
4 signature, and combining the second data item and the
5 second digital signature are performed in response to a
6 determination that the integrity of the first digital
7 signature may soon become able to be compromised.

Docket No. 2001-088-NSC

1 19. The computer program product of claim 17, comprising
2 additional functional descriptive data that, when
3 executed by the computer, enables the computer to perform
4 additional acts including:

5 writing the second timestamp to a storage medium.

1 20. The computer program product of claim 19, comprising
2 additional functional descriptive data that, when
3 executed by the computer, enables the computer to perform
4 additional acts including:

5 writing the first timestamp to the storage medium.

1 21. The computer program product of claim 19, wherein
2 the storage medium is memory.

1 22. The computer program product of claim 19, wherein
2 the storage medium is one of a disk and tape.

1 23. A computer program product in a computer readable
2 medium, for upgrading the integrity of a first timestamp
3 of a document, wherein the first timestamp includes a
4 first hash value computed with a first hash function,
5 comprising functional descriptive data that, when
6 executed by a computer, enables the computer to perform
7 acts including:

8 calculating a second hash value of the document
9 using a second hash function;

10 combining the second hash value with a current time
11 value to form a data item;

12 computing a digital signature of the data item; and

Docket No. 2001-088-NSC

13 combining the digital signature and the data item to
14 form a second timestamp.

1 24. The computer program product of claim 23, wherein
2 computing the second hash value, combining the second
3 hash value with the current time value, computing the
4 digital signature, and combining the data item with the
5 digital signature are performed in response to a
6 determination that the integrity of the first hash value
7 may soon become able to be compromised.

1 25. The computer program product of claim 23, comprising
2 additional functional descriptive data that, when
3 executed by the computer, enables the computer to perform
4 additional acts including:
5 writing the second timestamp to a storage medium.

1 26. The computer program product of claim 25, comprising
2 additional functional descriptive data that, when
3 executed by the computer, enables the computer to perform
4 additional acts including:
5 writing the first timestamp to the storage medium.

1 27. The computer program product of claim 25, wherein
2 the storage medium is memory.

1 28. The computer program product of claim 25, wherein
2 the storage medium is one of a disk and tape.

Docket No. 2001-088-NSC

1 29. A computer program product in a computer-readable
2 medium, for verifying the integrity of an upgrade
3 timestamp associated with an earlier timestamp,
4 comprising functional descriptive data that, when
5 executed by a computer, enables the computer to perform
6 acts including:

7 verifying integrity of a first digital signature
8 associated with the upgrade timestamp;
9 calculating a first hash value of a second digital
10 signature associated with the earlier timestamp; and
11 verifying that the first hash value matches a second
12 hash value associated with the upgrade timestamp.

1 30. The computer program product of claim 29, comprising
2 additional functional descriptive data that, when
3 executed by the computer, enables the computer to perform
4 additional acts including:

5 verifying integrity of the earlier timestamp.

1 31. The computer program product of claim 30, wherein
2 verifying the integrity of the earlier timestamp
3 includes:

4 verifying integrity of the second digital signature;
5 calculating a third hash value of a document
6 associated with the earlier timestamp; and
7 verifying that the third hash value matches a fourth hash
8 value associated with the earlier timestamp.

1 32. A computer program product in a computer-readable
2 medium, comprising functional descriptive data that, when

2001-088-NSC

Docket No. 2001-088-NSC

3 executed by a computer, enables the computer to perform
4 acts including:
5 verifying integrity of each of a plurality of
6 digital signatures, wherein each of the plurality of
7 digital signatures signs a timestamp, and each timestamp
8 includes a hash value of a common document, each hash
9 value having been calculated with a different hash
10 function.

1 33. A data processing system for upgrading the integrity
2 of a first timestamp having a first digital signature,
3 comprising means for:
4 computing a hash value of the first digital
5 signature;
6 combining the hash value with a current time value
7 to form a second data item;
8 computing a second digital signature based on the
9 second data item; and
10 combining the second data item and the second digital
11 signature to form a second timestamp.

1 34. The data processing system of claim 33, wherein
2 computing the hash value, combining the hash value with
3 the current time value, computing the second digital
4 signature, and combining the second data item and the
5 second digital signature are performed in response to a
6 determination that the integrity of the first digital
7 signature may soon become able to be compromised.

Docket No. 2001-088-NSC

1 35. The data processing system of claim 33, comprising
2 additional means for writing the second timestamp to a
3 storage medium.

1 36. The data processing system of claim 35, comprising
2 additional means for writing the first timestamp to the
3 storage medium.

1 37. The data processing system of claim 35, wherein the
2 storage medium is memory.

1 38. The data processing system of claim 35, wherein the
2 storage medium is one of a disk and tape.

1 39. A data processing system for upgrading the integrity
2 of a first timestamp of a document, wherein the first
3 timestamp includes a first hash value computed with a
4 first hash function, the data processing system
5 comprising means for:
6 calculating a second hash value of the document
7 using a second hash function;
8 combining the second hash value with a current time
9 value to form a data item;
10 computing a digital signature of the data item; and
11 combining the digital signature and the data item to
12 form a second timestamp.

1 40. The data processing system of claim 39, wherein
2 computing the second hash value, combining the second
3 hash value with the current time value, computing the

Docket No. 2001-088-NSC

4 digital signature, and combining the data item with the
5 digital signature are performed in response to a
6 determination that the integrity of the first hash value
7 may soon become able to be compromised.

1 41. The data processing system of claim 39, comprising
2 additional means for writing the second timestamp to a
3 storage medium.

1 42. The data processing system of claim 41, comprising
2 additional means for writing the first timestamp to the
3 storage medium.

1 43. The data processing system of claim 41, wherein the
2 storage medium is memory.

1 44. The data processing system of claim 41, wherein the
2 storage medium is one of a disk and tape.

1 45. A data processing system for verifying the integrity
2 of an upgrade timestamp associated with an earlier
3 timestamp, comprising means for:

4 verifying integrity of a first digital signature
5 associated with the upgrade timestamp;
6 calculating a first hash value of a second digital
7 signature associated with the earlier timestamp; and
8 verifying that the first hash value matches a second
9 hash value associated with the upgrade timestamp.

Docket No. 2001-088-NSC

1 46. The data processing system of claim 45, comprising
2 additional means for:
3 verifying integrity of the earlier timestamp.

1 47. The data processing system of claim 46, wherein
2 verifying the integrity of the earlier timestamp
3 includes:
4 verifying integrity of the second digital signature;
5 calculating a third hash value of a document
6 associated with the earlier timestamp; and
7 verifying that the third hash value matches a fourth
8 hash value associated with the earlier timestamp.

1 48. A data processing system comprising means for:
2 verifying integrity of each of a plurality of
3 digital signatures, wherein each of the plurality of
4 digital signatures signs a timestamp, and each timestamp
5 includes a hash value of a common document, each hash
6 value having been calculated with a different hash
7 function.